

# Índice

---

<b>Índice .....</b>	<b>V</b>
<b>Índice de figuras.....</b>	<b>IX</b>
<b>Prólogo .....</b>	<b>XIII</b>
<b>1 Introducción .....</b>	<b>1</b>
<b>2 Redes WLAN: Aspectos básicos .....</b>	<b>3</b>
<b>2.1 Arquitecturas o topologías de red WLAN .....</b>	<b>4</b>
2.1.1 Modo IBSS .....	10
2.1.2 Modo BSS .....	11
2.1.3 Modo ESS .....	11
<b>2.2 Labores de estandarización .....</b>	<b>17</b>
2.2.1 Breve historia.....	17
2.2.2 Wi-fi Alliance .....	18
2.2.3 Bandas de frecuencias de las redes wlan .....	19
2.2.4 Familia de estándares ieee802.11 .....	21
2.2.5 Estándares de capa física y de enlace .....	22
2.2.6 Estándares de optimización .....	24
<b>3 Ataques en redes WLAN al detalle .....</b>	<b>30</b>
<b>3.1 Ataques pasivos .....</b>	<b>30</b>
3.1.1 Espionaje/Surveillance .....	30
3.1.2 Escuchas/Sniffing/Eavesdropping .....	30
3.1.3 Wardriving.....	31
3.1.4 Warchalking.....	32
3.1.5 Ataques de descubrimiento de contraseña .....	33
3.1.6 Descubrimiento de ESSID ocultos .....	35
<b>3.2 Ataques activos .....</b>	<b>36</b>
3.2.1 Puntos de acceso no autorizados/Rogue APs .....	36
3.2.2 Spoofing .....	37
3.2.3 Man In The Middle.....	39
3.2.4 Secuestro de sesiones / Hijacking.....	40
3.2.5 Denegación de servicio (DOS)/Jamming.....	40
<b>4 Mecanismos de seguridad al detalle .....</b>	<b>43</b>
<b>4.1 Mecanismos de seguridad del nivel de enlace IEEE 802.11 .....</b>	<b>43</b>
4.1.1 PPTP .....	44
4.1.2 L2TP .....	45
4.1.3 WEP .....	46
4.1.4 WPA .....	52
4.1.5 IEEE 802.11i.....	57
4.1.6 WPA2 .....	59

4.1.7 Autenticación y gestión de claves de WPA, WPA2 e IEEE 802.11i: EAP e IEEE 802.1x .....	60
<b>4.2 Mecanismos de seguridad del nivel de red .....</b>	<b>74</b>
4.2.1 IPsec VPN .....	74
<b>4.3 Mecanismos de seguridad del nivel de transporte .....</b>	<b>79</b>
4.3.1 SSL/TLS .....	79
4.3.2 SSL VPN.....	86
<b>4.4 Mecanismos de seguridad del nivel de aplicación .....</b>	<b>92</b>
4.4.1 SSH .....	92
4.4.2 HTTPS .....	93
<b>4.5 Conclusiones .....</b>	<b>95</b>
4.5.1 Seguridad en el modelo OSI .....	95
4.5.2 Comparativa entre diferentes mecanismos de seguridad .....	97
4.5.3 Comparativa de los mecanismos de seguridad frente a ataques en redes WLAN .....	100
4.5.4 Conclusiones .....	104
<b>5 Recomendaciones de diseño para redes privadas empresariales .....</b>	<b>105</b>
<b>5.1 Normas de diseño básicas .....</b>	<b>105</b>
5.1.1 Recomendaciones de ingeniería social.....	105
5.1.2 Recomendaciones de red.....	105
5.1.3 Recomendaciones de protección física de la señal .....	109
<b>5.2 Soluciones de seguridad en entorno empresarial .....</b>	<b>110</b>
5.2.1 WEP .....	110
5.2.2 WPA .....	112
5.2.3 Combinación de los mecanismos de seguridad WEP y WPA .....	115
5.2.4 IEEE 802.11i.....	115
5.2.5 IPsec VPN .....	116
<b>6 Recomendaciones de diseño para redes WLAN públicas.....</b>	<b>121</b>
<b>6.1 Normas de diseño básicas .....</b>	<b>121</b>
6.1.1 Recomendaciones de ingeniería social dirigidas al usuario. ....	121
6.1.2 Recomendaciones de red.....	122
<b>6.2 Soluciones de seguridad en entorno público.....</b>	<b>123</b>
6.2.1 Autenticación de usuarios mediante el método de autenticación universal (UAM): Portal cautivo .....	123
6.2.2 Autenticación de usuarios mediante de tarjeta SIM .....	127
6.2.3 Agregadores de Hotspots o de redes WLAN: iPass, Boingo y GoRemote .....	128
<b>7 Seguridad en redes WLAN del hogar .....</b>	<b>137</b>
<b>7.1 Normas de diseño básicas .....</b>	<b>138</b>
7.1.1 Recomendaciones de ingeniería social.....	138
7.1.2 Recomendaciones de red.....	138
7.1.3 Recomendaciones de protección física de la señal .....	140
<b>7.2 Soluciones de seguridad en redes del hogar .....</b>	<b>140</b>
7.2.1 WEP .....	141
7.2.2 WPA-PSK .....	143

<b>8 Definiciones útiles .....</b>	<b>145</b>
<b>9 Acrónimos.....</b>	<b>153</b>
<b>10 Referencias y bibliografía.....</b>	<b>157</b>

## Índice de figuras

---

Figura 1 Punto de acceso.....	4
Figura 2 Modo de operación de un punto de acceso .....	5
Figura 3 Creación de tabla de asociación de direcciones MAC y puertos: paso 1.....	6
Figura 4 Creación de tabla de asociación de direcciones MAC y puertos: paso 2.....	6
Figura 5 Creación de tabla de asociación de direcciones MAC y puertos: paso 3.....	7
Figura 6 Puntos de acceso inalámbricos.....	7
Figura 7 Ejemplos de estaciones inalámbricas .....	8
Figura 8 Red WLAN en modo ad-hoc .....	8
Figura 9 Red WLAN en modo infraestructura .....	9
Figura 10 Topologías de red WLAN: IBSS (Independent Service Set).....	10
Figura 11 Topologías de red WLAN: BSS (Basic Service Set) .....	11
Figura 12 Topologías de red WLAN: ESS (Extended Service Set) .....	12
Figura 13 Topologías de red WLAN: Sistemas de distribución WDS y LAN .....	13
Figura 14 Topologías de red WLAN: Sistemas de distribución propietarios.....	13
Figura 15 Topología de una red Mesh.....	14
Figura 16: Arquitectura distribuida.....	16
Figura 17: Arquitectura centralizada (Wireless Switch) .....	16
Figura 18 Sello que contienen los productos certificados por la Wi-Fi Alliance.....	18
Figura 19 Ejemplo de búsqueda de equipos certificados Wi-Fi por la Wi-Fi Alliance.....	19
Figura 20 Número de canales en la banda de 2,4GHz .....	20
Figura 21 El modelo OSI y el protocolo 802.11 .....	21
Figura 22 Estándares WLAN a nivel físico. ....	22
Figura 23 Procedimiento del estándar IEEE802.11k.....	27
Figura 24 Wardriving .....	31
Figura 25 Warchalking.....	32
Figura 26 Escenario de un ataque de descifrado de clave WEP .....	34
Figura 27 Escaneo pasivo de redes WLAN.....	35
Figura 28 Escaneo activo de redes WLAN.....	36
Figura 29 Validadores suplantables mediante spoofing .....	37
Figura 30 Ataque de spoofing.....	38
Figura 31 Ataque ARP Man In The Middle .....	40
Figura 32 Ataque de secuestro de sesiones .....	41
Figura 33 Mecanismos de seguridad existentes en las distintas capas de OSI.....	43
Figura 34 Autenticación y asociación en una red WLAN.....	47
Figura 35 Shared Key Authentication: proceso de autenticación .....	48
Figura 36 Clave WEP de 40 bits con valores ASCII .....	49
Figura 37 Generación de clave WEP mediante algoritmo PRNG .....	49
Figura 38 Clave WEP de 40 bits con valores hexadecimales .....	50
Figura 39 Proceso de cifrado WEP de la información .....	51
Figura 40 Proceso de descifrado WEP de la información .....	51
Figura 41 Generación dinámica de clave por paquete.....	56
Figura 42 Formato de trama WPA.....	57

Figura 43 Principales diferencias entre WPA y IEEE 802.11i.....	59
Figura 44 Autenticación IEEE 802.1x + EAP: pila de protocolos.....	61
Figura 45 Autenticación WLAN: arquitectura IEEE 802.1x.....	62
Figura 46 Autenticación RADIUS basada en EAP .....	65
Figura 47 Funcionamiento de EAP-TTLS.....	69
Figura 48 Autenticación mediante SIM: Arquitectura.....	70
Figura 49 Intercambio de tramas durante la autenticación EAP-SIM.....	71
Figura 50 Modos de funcionamiento IPsec: modo transporte y modo túnel .....	78
Figura 51 Intercambio de mensajes para el establecimiento de un canal seguro SSL.....	81
Figura 52. Esquema general de una solución SSL VPN .....	87
Figura 53. Redireccionadores de protocolos.....	88
Figura 54. Protocolos IPsec y SSL en la arquitectura de protocolos OSI .....	91
Figura 55 Autenticación UAM: Intercambio de mensajes RADIUS .....	93
Figura 56 Mecanismos de seguridad existentes en las distintas capas de OSI.....	95
Figura 57 Comparación de diferentes mecanismos de seguridad de redes WLAN IEEE 802.11i con diferentes métodos EAP e IPsec VPN: Seguridad vs. Coste de gestión.....	103
Figura 58 Arquitectura básica de una red WLAN .....	107
Figura 59 Arquitectura de seguridad con WEP .....	111
Figura 60 Arquitectura de seguridad con WPA.....	113
Figura 61 Arquitectura de seguridad con WPA.....	116
Figura 62 Diseño de una arquitectura basada en VPN IPsec .....	118
Figura 63 Autenticación UAM: Arquitectura .....	124
Figura 64 Autenticación UAM: Intercambio de mensajes RADIUS .....	125
Figura 65 Autenticación mediante SIM: ejemplos de dispositivos de usuario .....	127
Figura 66 Autenticación mediante SIM: Arquitectura.....	128
Figura 67 Boingo .....	129
Figura 68 iPassConnect™ Universal.....	129
Figura 69 GoRemote .....	130
Figura 70 Aplicativo o Software de usuario Boingo .....	131
Figura 71 Software de usuario iPassConnect™ Universal.....	132
Figura 72 Arquitectura del sistema iPass para autenticación de usuarios en red corporativa .....	133
Figura 73 Soluciones GoRemote .....	134
Figura 74 Software de usuario de roaming GoRemote .....	135
Figura 75 Posibles arquitecturas de redes WLAN en el hogar.....	141
Figura 76 Arquitectura de seguridad de una red WLAN en el hogar con WEP.....	142
Figura 77 Arquitectura de seguridad en una red WLAN en el hogar con WPA-PSK.....	144

## Índice de tablas

Tabla 1 Descripción general de las capas físicas 802.11 .....	23
Tabla 2 Estándares físicos y de optimización .....	24
Tabla 3 Modos de certificación WPA y WPA2 .....	55
Tabla 4 Síntesis EAP .....	66
Tabla 5 Características de diferentes métodos EAP .....	73
Tabla 6 Protocolos que operan sobre SSL .....	84
Tabla 7 Aplicaciones que pueden ser soportadas sin la necesidad de emplear usuario.....	90
Tabla 8. Aplicaciones que se pueden soportar mediante el uso de usuario .....	90
Tabla 9 Comparativa: WEP, WPA, IEEE 802.11i e IPsec VPN .....	97
Tabla 10 Resumen mecanismos de seguridad 802.11 vs. ataques a redes 802.11 .....	101